Le passeport électronique

Les pays de l'Union européenne ont décidé d'introduire un nouveau type de passeports afin de réduire de façon significative le risque de fraude et de falsification. Ce passeport est équipé d'une puce à radiofréquence qui remplacera le passeport "classique".
Le ministre de l'intérieur a donc saisi le 10 Octobre 2005 la Commission Nationale de l'informatique et des Libertés (CNIL) d'un projet de décret instituant le passeport électronique et des modifications du traitement de données à caractère personnel DELPHINE permettant l'établissement, la délivrance et la gestion des passeports.
La mise en œuvre du passeport est soumise à l'autorisation de la CNIL. Créée par la loi du 6 Janvier 1978 la CNIL est une autorité administrative indépendante. Elle est composé de 17 membres soit deux députés, deux sénateurs, deux membres du conseil économique et social, du conseil d'Etat, de la Cour de Cassation et de la Cour des comptes, et cinq personnes qualifiées nommées par décret. C'est un organe consultatif chargé de rendre des conseils et avis auprès des autorités publiques et professionnels qui peuvent la solliciter. Elle veille à ce que tous traitements de données à caractère personnel soient mis en œuvre conformément à la loi. Elle peut autoriser ou refuser la création de fichiers dangereux. Elle détient également un pouvoir réglementaire limité en établissant les normes que les fichiers devront respecter et les règlements types qui assurent la sécurité des systèmes. La CNIL est ainsi compétente pour se positionner sur ce nouveau système d'identification.

Le concept du passeport électronique est né dans le cadre des mesures prises par les Etats-Unis au lendemain des attaques terroristes du 11 septembre 2001. Les contrôles aux frontières ont ainsi été renforcés. Désormais toutes personnes étrangères souhaitant entrer dans le pays s'y verront refuser l'accès, si elle ne dispose pas d'un permis de séjour valable. Toutefois les ressortissants de certains pays ont été exemptés de cette obligation, sous condition qu'ils disposent d'un passeport pouvant être lu de façon automatisée. Michael Chertoff, ministre américain de la Sécurité intérieure a affirmé que ces passeports représentaient « *une avancée significative pour que des terroristes n'utilisent pas des passeports perdus ou volés pour entrer aux États-Unis* ».
Aujourd'hui l'Europe a fait du passeport électronique une réelle priorité suite aux attentats de Madrid de mars 2004 et ceux de Londres de juillet 2005. Le caractère obligatoire de ce nouveau système ne se limite plus aux seuls voyageurs destinataires des Etats-Unis, mais s'étend maintenant à toutes personnes qui veulent faire une demande d'obtention ou de renouvellement de passeport.
La France est en retard dans la mise en place du passeport électronique dû à un contentieux juridique entre le Ministre de l'Intérieur et l'Imprimerie Nationale. En effet, ce passeport est rendu obligatoire depuis fin 2006, afin de pénétrer sur le territoire américain sans passer par l'obtention d'un visa.
Le 28 Août 2006 représentait la date butoir pour que les pays de l'Union Européenne se conforment au règlement européen du 13 décembre 2004. Seuls trois pays sur 27 n'ont pas encore adopté le passeport électronique c'est-à-dire l'Andorre, le Brunei et le Liechtenstein qui devront alors demander un visa pour entrer sur le sol américain.
Le passeport électronique comportera donc des données biométriques, c'est-à-dire la photographie numérisée et, dans un futur proche, l'empreinte digitale du détenteur.

Au vue de sa finalité, le passeport électronique n'est-il pas une avancée technologique trop risqué pour la préservation des libertés individuelles de chacun ?

S'il apparaît que le passeport électronique soit une nouvelle technologie en phase avec l'évolution de la société (I), il est cependant largement remis en cause suite aux nombreuses polémiques qu'il a suscité (II).

I) La création d'une nouvelle technologie en phase avec l'évolution de la société

Le passeport électronique est à la fois un moyen permettant de prévenir et lutter contre toute forme de fraude actuelle (a), mais permet également de garantir les données personnelles propres à chaque individu (b).

a) Le passeport électronique, un moyen permettant de prévenir et de lutter contre toute forme de fraude actuelle

Selon la CNIL le premier objectif du passeport est « *de prévenir et lutter contre la fraude documentaire portant sur ces titres grâce à de nouvelles modalités de production, à l'insertion dans ce passeport de la photographie numérisée de son détenteur et d'un composant électronique (puce sans contact) contenant des données relatives à son détenteur et à sa délivrance, ainsi qu'à la mise en place de transmissions de données relatives aux passeports volés ou perdus vers le Système d'information Schengen et vers Interpol.* »

Le projet de décret envisage de rendre les données du fichier national des passeports accessibles aux services chargés de la lutte anti-terroriste de la police et de la gendarmerie nationale dans le cadre de leurs missions. La CNIL estime qu'il est nécessaire qu'il figure dans le projet de décret, « *la liste des données accessibles strictement nécessaires à la poursuite des finalités de lutte anti-terroriste, l'énumération des services de police et de gendarmerie destinataires des données ainsi que les mesures propres à assurer la sécurité des données à l'occasion de leur consultation, et notamment les modalités d'habilitation d'accès et de contrôle systématique des consultations du fichier national des passeports* ».
Elle demande d'autant plus, qu'une personne soit désignée auprès du directeur général de la police, pour assurer le contrôle effectif des accès des services chargé de la lutte anti-terroriste, ainsi que la transmission à la CNIL d'un bilan annuel des contrôles opérés sur ces accès.
La lutte contre les fraudes et le terrorisme est le principal objectif de la création de ce passeport. Par le biais du passeport l'accessibilité des fichiers nationaux va devenir plus simple et permettra une meilleure efficacité dans le travail pour les services concernés.

En outre, le système d'information Schengen et le système d'information Interpol vont être en connexion avec le fichier national des passeports ainsi que les fichiers des personnes recherchées.
Le système d'information Schengen est un système d'information utilisé dans certains pays européens , qui peuvent y consulter ou y enregistrer des informations sur des personnes ou des objets. Les données concernent par exemple des personnes sous mandat d'arrêt ou des objets dont on a perdu la trace. Quant au système d'information d'Interpol il s'agit d'une organisation internationale sur la coopération policière internationale qui étudie et analyse la criminalité et le terrorisme.
Ils mettront également tous deux en place la transmission de données relatives aux passeports volés ou perdus. Ainsi le passeport électronique peut être considéré comme une mesure nécessaire et importante quant à l'aide apportée à la lutte contre les fraudes et le terrorisme.

Enfin, le passeport électronique permet la simplification de la vie quotidienne des administrés en devenant un document qui pourra être présenté à l'occasion de toute

démarche nécessitant la justification de son identité. La CNIL nous indique qu'il pourra ainsi être utilisé dans la sphère publique par exemple lors des démarches auprès des services de l'Etat, des collectivités territoriales ou des organismes de sécurité sociale mais également dans la sphère privé pour l'ouverture d'un compte bancaire par exemple.
Les mesures techniques prises en gage de sécurité sont de nature à garantir l'authentification, la confidentialité et l'intégrité des données enregistrées sur le composant électronique du passeport. Le passeport permettra d'identifier avec certitude son titulaire.

b) Le passeport électronique, nouveau système d'identification garantissant les données personnelles propres à l'individu

La CNIL énumère dans sa délibération différentes garanties mise en place par le ministère de l'intérieur.
Elle nous explique que le passeport contiendra une photographie numérisée de son détenteur et une puce électronique contenant des données relatives à son détenteur. Le passeport aura la valeur d'un titre d'identité équivalent à la carte d'identité nationale.
Ainsi, le passeport électronique est identique au passeport conventionnel, mais il contient en plus une puce RFID (radio frequency identification). On reconnaît un passeport RFID au logo graphique présent sur la page de couverture.

Dans sa version actuelle cette puce RFID contient les informations générales sur l'identité du porteur c'est-à-dire le nom, prénom, date de naissance etc ainsi qu'une photo d'identité numérisé. Il est prévu qu'en 2009 une copie numérique des empreintes digitales du porteur soit ajoutée. Le fonctionnement de cette puce (ainsi que celui de tous les passeports émis par les différents pays du monde) est compatible avec les caractéristiques définies par l'Organisation de l'Aviation Civile Internationale (OACI). L'OACI est une organisation internationale qui dépend des Nations unies. Son rôle est de participer à l'élaboration des normes qui permettent la standardisation du transport aéronautique international. Ces caractéristiques prévoient que la puce puisse également stocker une empreinte de l'iris de l'œil.

La Commission observe qu'une telle technologie est pour la première fois utilisée en France dans le cadre de documents d'identité et qu'elle appelle à la mise en place de sécurités particulières.
La commission relate les différentes sécurités développées, afin de garantir l'authentification, la confidentialité et l'intégrité des données enregistrées sur le composant électronique du passeport. En effet, la lecture des données suppose l'ouverture physique du passeport, la lecture optique suppose un équipement spécialisé, une session de sécurité est alors ouverte et le numéro de session est aléatoire pour écarter toutes possibilités de tracer les personnes.

La Commission précise que le futur passeport est composé d'une puce sans contact permettant sous certaines conditions la lecture à faible distance des données relatives au détenteur du titre qui y sont enregistrées. Elle souligne également que ce passeport ne peut être lu que quand il se trouve ouvert. Mais elle poursuit en indiquant que tel ne sera pas le cas, si le passeport est présenté à un professionnel disposant du matériel de lecture adéquate.
Les données incluses dans le passeport peuvent être lues par le biais d'un lecteur optique de type « Delphine » ; le passeport électronique étant équipé d'une puce à radiofréquence, il pourra être lu sans contact physique direct avec le lecteur. Les échanges de données entre

la puce et le lecteur seront cryptés et le contenu de la puce sera limité aux informations figurant déjà sur le passeport.

Pour des raisons de sécurité un centre de personnalisation du passeport va être mis en place et confié à un sous-traitant, afin de produire les passeports de façon centralisés et non plus localement.
Un stockage provisoire des données doit intervenir, identique à celui mis en place pour la production actuelle de la carte nationale d'identité. La Commission ajoute qu'un engagement contractuel du prestataire est exigé par le ministère de l'intérieur, afin de préserver la sécurité des données traitées et surtout ne pas les utiliser à des fins détournées. Elle précise en plus que les données ne seront pas conservées plus de trois mois par le prestataire, afin d'assurer la protection des données à caractère personnel ainsi traitées. Elle rappelle enfin que tout accès frauduleux est pénalement répréhensible par les articles 226-15 et 432-9 du Code pénal.

Le règlement européen du 13 décembre 2004 affirme que pour mieux sécuriser le passeport, celui-ci sera composé d'une photographie numérisée et de l'intégration d'identification biométriques. La photo est donc la seule donnée "biométrique" du passeport à l'heure actuelle. La biométrie signifie l'identification certaine d'un individu à partir de caractéristiques biomorphologiques c'est-à-dire empreintes digitales, iris, ADN, traits du visage, voix etc permettant de faire échec aux falsifications ou usurpations d'identité par exemple.
La photographie du détenteur du titre ne sera pas enregistrée dans le fichier national des passeports, elle sera numérisée par les services préfectoraux avant d'être envoyée au prestataire de service, et d'être détruite au plus tard trois mois à compter de la réception de l'ordre de production.

Le passeport électronique est difficile à falsifier car les informations stockées sur la puce RFID sont signées numériquement c'est-à-dire que chaque pays émetteur dispose d'une Autorité de Certification racine (AC). Il est donc possible de vérifier que la signature du passeport est valide et a été apposée par une entité approuvée par l'autorité du pays émetteur.

Cependant malgré une technologie qui apparait pour le moins sécurisante le passeport électronique suscite de nombreux débats et ne paraît pas aussi infaillible qu'on croit.

II) Une remise en cause du passeport électronique suite aux nombreuses polémiques

Les premiers passeports électroniques ont été diffusés en France le 13 Avril 2006 provoquant de nombreuses inquiétudes d'une part du fait des possibilités d'atteinte à la vie personnelle (a), et d'autre part par la fiabilité (sécurité) du passeport (b).

a) *Des atteintes portées aux libertés individuelles*

Certaines associations dénoncent une atteinte faites aux libertés individuelles. C'est le cas de la Ligue des droits de l'Homme, qui a lancé une pétition contre ce projet soulignant le risque d'un « *fichage généralisé de la population française* ».

Le passeport électronique comporte des risques accrus d'atteinte à la vie privée.

Il y a un risque de traçage des voyageurs dans la mesure où le passeport électronique semble faciliter l'enregistrement systématique de tous les voyageurs étant donné que le passeport est informatisé, la personne est donc "suivie". Mais en réalité, ce risque existait déjà avec le passeport traditionnel, car celui-ci est équipé depuis plusieurs années d'une zone lisible par une machine la MRZ (Machine Readable Zone) qui dès que l'on passe le passeport dans un lecteur optique transmet à un ordinateur les informations sur l'identité du porteur.

Les données biométriques stockées sur la puce du passeport peuvent être exposées à des risques d'abus éventuels, étant donné qu'elles peuvent également comporter des informations supplémentaires susceptibles d'être "sensibles" par exemple des informations sur l'état de santé ou l'origine raciale de la personne concernée. La CNIL a assurée que les données biométriques seront supprimées dans un délai de trois mois après la remise du passeport à son titulaire.

Tout changement demandé par le titulaire (après un mariage par exemple) nécessitera le renouvellement complet du document. Ce qui implique alors une dépense de 60 euros en timbres fiscaux.

Le 12 janvier 2006, la CNIL a donné sa position dans le cadre d'une affaire où une clinique souhaitait utiliser un dispositif biométrique de reconnaissance de l'empreinte digitale ayant pour finalité le contrôle des horaires des employés. Elle estime que « *les empreintes digitales sont des données biométriques qui laissent des traces pouvant ensuite être exploitées à des fins d'identification de personnes* ». Elle déclare que les données associées à des empreintes digitales comportent un risque d'atteinte aux libertés individuelles dans la mesure où ces bases sont susceptibles d'être utilisées à des fins étrangères à la finalité initialement poursuivie. La Commission déclare que « *la constitution de bases de données d'empreintes digitales, compte tenu des caractéristiques d'élément d'identification physique retenu et des usages possibles de ces bases de données, ne peut être admise que dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse* ».
La CNIL émet cependant quelques réserves concernant le système biométrique notamment sur l'empreinte digitale qui pourrait être susceptible d'utilisation à des fins étrangères. En effet dans une délibération du 28 décembre 2007, la CNIL s'est positionnée sur l'utilisation du dispositif de biométrie dans le passeport électronique en plus de la photographie numérisée. Son analyse repose sur le fait que « *l'empreinte digitale est une biométrie à trace* », et que « *ces traces peuvent être capturées à l'insu des personnes et être utilisées notamment pour usurper leur identité* ». La CNIL reconnaît donc le risque des passeports électroniques.
La CNIL est plus favorable aux dispositifs où l'empreinte digitale est enregistrée exclusivement sur un support individuel par exemple carte à puce, clé USB, et non dans une base centralisée.

Le passeport électronique en plus de porter atteinte à certaines libertés individuelles n'est pas aussi sécurisant qu'il ne pourrait paraître.

b) Une sécurité faillible

S'il apparaît que le passeport électronique soit d'une sécurité remarquable il n'en est pas pour autant infaillible. En effet plusieurs situations nous démontrent le contraire.

Théoriquement il n'est pas possible de lire le contenu de la puce RFID sans avoir accès aux informations par une machine spécifique, mais il est par contre toujours possible de détecter à distance si quelqu'un porte sur lui un passeport électronique. Il est probablement aussi possible de reconnaître le type de passeport par exemple la nationalité du porteur en fonction du type de puce RFID et de sa façon de répondre aux sollicitations. Théoriquement, la puce d'un passeport électronique n'est interrogeable qu'à une dizaine de centimètres. Cependant, en amplifiant le lecteur, certaine sources indiquent que cette distance pourrait être portée à plusieurs mètres. Ainsi, il pourrait être possible de réaliser des attentats où une bombe se déclencherait à l'approche d'une victime portant un passeport d'une nationalité donnée.
Afin de limiter la possibilité d'une lecture à distance du passeport, la CNIL a inséré dans une des pages de la couverture du passeport une trame métallique qui empêche la lecture si le passeport n'est pas ouvert, l'ouverture physique du passeport est ainsi une réelle garantie. Le passeport américain dispose également de cette protection alors que le passeport anglais lui n'en bénéficie pas.

Les données stockées sur la puce RFID sont protégées par un mécanisme de sécurité appelé le BAC (Basic Access Control). Ce mécanisme de sécurité peut être brisé. Le principe du BAC est que la puce RFID n'accepte de transmettre les données qu'elle contient qu'à un lecteur RFID qui est capable de lui donner une clé secrète.
La protection BAC n'est pas réputée pour son efficacité. Il peut être possible de lire illégalement le contenu de la puce RFID sans avoir lu les données par la bande MRZ. En particulier, si l'on devine certaines des données MRZ (par exemple le nom du porteur, sa date de naissance, etc…), il devient alors possible de réaliser des attaques en essayant toutes les valeurs possibles de la MRZ. Ces attaques ont déjà eu lieu, l'une d'elles a été commentée en mars 2007 dans le journal anglais "The Daily Mail". Cependant il faut tout de même relativiser puisque selon le Daily Time il aurait fallu plusieurs heures aux attaquants pour réaliser cette infraction.

Un passeport peut être également cloné.
Plusieurs sources ont indiqué qu'elles pouvaient facilement cloner la puce RFID d'un passeport. Le principe du clonage est simple : il suffit d'avoir le passeport, de lire le contenu de la puce RFID après avoir pris connaissance du MRZ, puis d'inscrire les données lues sur une seconde puce RFID (le clone). Il n'est cependant pas possible de modifier les données qui seront inscrites sur le clone, car la signature électronique de la puce deviendrait alors invalide.
Cette possibilité de cloner la puce n'a jamais été formellement démentie.

En outre l'efficacité des contrôles n'est pas certain puisque tous les postes de contrôle ne sont pas équipés de systèmes de reconnaissance faciale qui permet la vérification de la photo stockée dans le passeport correspondant bien à la personne contrôlée, le passeport électronique ne permet donc pas de vérifier avec certitude l'identité du porteur.

Enfin le contrôle d'accès de base comporte un degré de sécurisation de 56 Bit qui se trouve être assez réduit, certaines données peuvent donc être déduites ou simplement calculées. Ainsi, si les numéros de passeport sont attribués de façon continue et qu'une personne connaît le nombre approximatif de passeports issus par mois, celle-ci pourrait considérablement réduire le nombre de combinaisons possibles. Des essais, réalisés aux Pays-Bas, ont démontré que le degré de sécurité pourrait ainsi être réduit à 35 Bit. De nos jours, un ordinateur standard pourrait calculer ce nombre de combinaisons dans un délai de quelques heures.